CLAIM AMENDMENTS

Claims 1-21 are pending, wherein claims 4-21 are newly added by this amendment.

1. (original) A MAC (media access control) address-based communication restricting method comprising the steps of:

receiving packet data upon request of communication through at least one port of a plurality of ports of an Ethernet switch;

reading a MAC destination address and a MAC source address included in the received packet data;

detecting, in an address table, access vectors corresponding to the MAC destination and source addresses; and

denying access if the access vectors of the MAC destination and source addresses are not matched.

2. (original) The method as set forth in claim 1, further comprising steps of:

configuring an anti-hacker table comprising information pertaining to a plurality of client nodes and a plurality of server nodes of a network, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address, and each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address;

determining whether the received MAC source address is stored in said address table;

8   configuring an address entry for said received MAC source address when it is determined that

9   said MAC source address is not stored in said address table and identifying said received MAC

10   source address as a new MAC source address;

11   determining whether said new MAC source address is stored in said anti-hacker table; and

12   storing the configured address entry for said received MAC source address in said address

13   table when it is determined that said new MAC source address is not stored in said anti-hacker table.

1   3. (original) The method as set forth in claim 2, further comprising steps of:

2   adding a port number, corresponding to the port through which said packet data was received,

3   to a storage area corresponding to said new MAC source address in said anti-hacker table, when it

4   is determined that said new MAC source address is stored in said anti-hacker table;

5   modifying an access vector included in said configured address entry for said new MAC

6   source address, to set security; and

7   storing the configured address entry including the modified access vector for said new MAC

8   source address in said address table.

1   4. (new) A packet switch restricting MAC (media access control) address-based

2   communication, comprising:

3   a host providing overall control to the packet switch and executing commands input to the

4   packet switch;

5   at least one MAC port performing MAC control operations and outputting a transmit/receive

6   command of a data packet;

7   a transmission/reception controller receiving said transmit/receive command;

8   a data exchange controlled by said transmission/reception controller, said data exchange

9   establishes paths of data and control signals between the host, the MAC port and a packet memory;

10   said packet memory storing received data packets, said packet memory including a port table

11   and an address table;

12   said port table storing information about a current status of the packet switch, port attributes

13   enable/disable, and packet reception completion of each MAC port; and

14   said address table storing registered MAC addresses, source access vectors corresponding

15   to source MAC addresses of said registered MAC addresses and destination access vectors

16   corresponding to destination MAC addresses of said registered MAC addresses.

1   5. (new) The packet switch as set forth in claim 4, said packet memory including further a

2   packet descriptor storing information about each packet stored in the packet memory.

1   6. (new) The packet switch as set forth in claim 5, wherein said packet information

2   comprises packet connection information.

1   7. (new) The packet switch as set forth in claim 4, further comprising a search memory

2   storing information by which a MAC port, corresponding to the destination MAC address of a

3   received data packet, is determined for data packet output.

8. (new) The packet switch as set forth in claim 7, wherein said transmission/reception controller temporarily stores received data packets, accesses said search memory, checks whether the destination MAC address in a header of the received data packet has been registered, locates where the registered destination MAC address is stored in the address table, and determines a MAC port through which the received data packet is to be output.

9. (new) The packet switch as set forth in claim 4, wherein said host includes an anti-hacker table comprising information pertaining to a plurality of client nodes and a plurality of server nodes of a network, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address, and each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address.

10. (new) The packet switch as set forth in claim 4, wherein said transmission/reception controller receives a data packet upon request of communication through the MAC port, reads the destination MAC address and source MAC address included in the received data packet, detects the destination access vector corresponding to the destination MAC address and the source access vector corresponding to the source MAC address, and denies the requested communication if the destination access vector and the source access vector do not match.

11. (new) The packet switch as set forth in claim 10, wherein said transmission/reception controller determines whether the received source MAC address is stored in said address table, configures an address entry for said received source MAC address when it is determined that said source MAC address is not stored in said address table and identifies said received source MAC address as a new source MAC address.

12. (new) The packet switch as set forth in claim 11, wherein said transmission/reception controller determines whether said new source MAC address is stored in said anti-hacker table, and stores the configured address entry for said received source MAC address in said address table when it is determined that said new source MAC address is not stored in said anti-hacker table.

13. (new) The packet switch as set forth in claim 11, wherein said transmission/reception controller adds a port number, corresponding to the MAC port through which said data packet was received, to a storage area corresponding to said new source MAC address in said anti-hacker table, when it is determined that said new MAC source address is stored in said anti-hacker table, modifies an access vector included in said configured address entry for said new source MAC address, to set security, and stores the configured address entry including the modified access vector for said new source MAC address in said address table.

14. (new) A method of restricting MAC (media access control) address-based communication through a packet switch, said method comprising steps of:

-6-

3 storing source MAC addresses and destination MAC addresses in an address table;

4 storing source access vectors in said address table, said source access vectors respectively

5 corresponding to said source MAC addresses;

6 storing destination access vectors in said address table, said destination access vectors

7 respectively corresponding to said destination MAC addresses;

8 comparing, upon receipt of a data packet, one of said source access vectors corresponding

9 to a source MAC address received in a header of said data packet, to one of said destination access

10 vectors corresponding to a destination MAC address received in said header of said data packet; and

11 preventing said MAC address-based communication when the compared source access vector

12 does not match the destination access vector.

1 15. (new) The method as set forth in claim 14, said comparing step comprising steps of:

2 extracting said source MAC address and said destination MAC address from said header of

3 said data packet;

4 determining whether said source MAC address and said destination MAC address are stored

5 in said address table; and

6 when it is determined that said source MAC address and said destination MAC address are

7 stored in said address table, reading the source access vectors corresponding to said source MAC

8 address and the destination access vectors corresponding to a destination MAC address from said

9 address table.

1   16. (original) The method as set forth in claim 15, further comprising a step of:

2   configuring an anti-hacker table comprising information pertaining to a plurality of client

3   nodes and a plurality of server nodes of a network, wherein each client node is identified by a

4   corresponding client MAC address, a corresponding host identification and a corresponding IP

5   (Internet protocol) address, and each server node is identified by a corresponding server MAC

6   address, a corresponding host identification and a corresponding IP (Internet protocol) address.

7   17. (new) The method as set forth in claim 16, further comprising steps of:

8   configuring an address entry for the extracted source MAC address when it is determined that

9   said source MAC address is not stored in said address table and identifying the extracted source

10   MAC address as a new source MAC address;

11   determining whether said new source MAC address is stored in said anti-hacker table; and

12   storing the configured address entry for said extracted source MAC addresses in said address

13   table when it is determined that said new source MAC address is not stored in said anti-hacker table.

1   18. (original) The method as set forth in claim 19, further comprising steps of:

2   adding a port number, corresponding to a port through which said data packet was received,

3   to a storage area corresponding to said new source MAC address in said anti-hacker table, when it

4   is determined that said new source MAC address is stored in said anti-hacker table;

5   modifying an access vector, included in said configured address entry, for said new source

6   MAC address, to set security; and

7   storing the configured address entry including the modified access vector for said new source

8   MAC address in said address table.

1   19. (new) A MAC (media access control) address-based communication restricting method

2   using access vectors stored in an address table, wherein the access vectors indicate whether two

3   nodes, corresponding to a source address and a destination address, may access each other, the

4   method comprising steps of:

5   receiving packet data upon request of communication through at least one port of a plurality

6   of ports of an Ethernet switch;

7   reading a received MAC destination address and a received MAC source address included

8   in the received packet data;

9   detecting, in the address table, an access vector corresponding to the received MAC

10   destination address and an access vector corresponding to the received MAC source address; and

11   denying access if the access vector of the received MAC destination address does not match

12   the access vector of the received MAC source address.

1   20. (new) The method as set forth in claim 19, further comprising steps of:

2   configuring an anti-hacker table comprising information pertaining to a plurality of client

3   nodes and a plurality of server nodes of a network, wherein each client node is identified by a

4   corresponding MAC address, a corresponding host identification and a corresponding IP (Internet

5   protocol) address, and each server node is identified by a corresponding MAC address, a

6   corresponding host identification and a corresponding IP (Internet protocol) address;

7   determining whether the received MAC source address is stored in said address table;

8   configuring an address entry for said received MAC source address when it is determined that

9   said received MAC source address is not stored in said address table and identifying said received

10   MAC source address as a new MAC source address;

11   determining whether said new MAC source address is stored in said anti-hacker table; and

12   storing the configured address entry for said received MAC source address in said address

13   table when it is determined that said new MAC source address is not stored in said anti-hacker table.

1   21. (new) The method as set forth in claim 20, further comprising steps of:

2   adding a port number, corresponding to the port through which said packet data was received,

3   to a storage area corresponding to said new MAC source address in said anti-hacker table, when it

4   is determined that said new MAC source address is stored in said anti-hacker table;

5   modifying an access vector included in said configured address entry for said new MAC

6   source address, to set security; and

7   storing the configured address entry including the modified access vector for said new MAC

8   source address in said address table.